**PRIORITY DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

09/786824

**Patent Office**
**Canberra**

EJHV

DE 99/2871

I, KIM MARSHALL, MANAGER EXAMINATION SUPPORT AND SALES, hereby certify that the annexed is a true copy of the Complete specification in connection with Application No. 43414/99 for a patent by ROBERT BOSCH GmbH filed on 05 August 1999.

# CERTIFIED COPY OF PRIORITY DOCUMENT

WITNESS my hand this Eighteenth
day of August 1999.

KIM MARSHALL
MANAGER EXAMINATION SUPPORT AND
SALES

Regulation 3.2

# AUSTRALIA

**Patents Act 1990**

COMPLETE SPECIFICATION

FOR A STANDARD PATENT

(ORIGINAL)

---

Name of Applicant: **ROBERT BOSCH GmbH** of Postfach 30 02 20, D-70442 Stuttgart, Germany

Actual Inventor(s):

Address for Service: **DAVIES COLLISON CAVE**, Patent Attorneys, of 1 Little Collins Street, Melbourne, Victoria 3000, Australia

Invention Title: **"A KEY CONTROL METHOD"**

Details of Associated Provisional Application No: PP5763/98

The following statement is a full description of this invention, including the best method of performing it known to us:

## A KEY CONTROL METHOD

The present invention relates to a key control method and a security system.

Passive security systems are available for vehicles which use remote keys having transponders that communicate with a transceiver of a vehicle, when the transponder is within range of the transceiver. Provided communication between a key and the transceiver follows a predetermined communications protocol, and unique authentication data is exchanged and validated, the key is considered a valid key and the system allows entry to and/or use of the vehicle. When the valid key subsequently moves out of range of the transceiver, the security system secures the vehicle by locking and immobilising the vehicle.

When a valid key for a vehicle becomes lost, the key needs to be deactivated so it can no longer be used to gain access to the vehicle. Accordingly, it is desired to a provide simple technique for deactivating lost keys and reactivating found valid keys, particularly when the keys are buttonless.

In accordance with the present invention there is provided a key control method for a security system having at least one valid key and electronic control means with a transceiver for communicating with said at least one valid key, said control means generating an authority for a secure object when authentication data is received from said at least one valid key and storing unique identification data for said at least one valid key, said method including accessing said unique identification data for said at least one valid key in a mode of said system;

characterised by storing enable data corresponding to said unique identification data for said at least one valid key, a user executing a predetermined procedure to enter a key validation mode of said system, and in said validation mode retaining said enable data for valid keys within range of said transceiver and deleting said enable data for valid keys which are out of range of said transceiver, whereby keys without said enable data are deactivated for said system.

The present invention also provides a security system including at least one valid key and electronic control means with a transceiver for communicating with said at least one valid

key, said control means generating an authority for a secure object when authentication data is received from said at least one valid key, and storing unique identification data for said at least one valid key, said system having a mode for accessing said unique identification data for said at least one valid key;

characterised in that said control means stores enable data corresponding to said unique identification data for said at least one valid key when activated for said system, and said control means enters a key validation mode when a user executes a predetermined procedure, and in said validation mode said enable data is retained for valid keys within range of said transceiver and deleted for valid keys out of range of said transceiver.

A preferred embodiment of the present invention is hereinafter described, by way of example only, with reference to the accompanying drawing, wherein:

Figure 1 is a block diagram of a preferred embodiment of a security system.

A security system, as shown in Figure 1, includes an electronic control unit (ECU) 2 which is mounted in a vehicle and includes processing circuitry to communicate with other electrical and electronic components of the vehicle and the security system. In particular, the ECU 2 includes an rf transceiver 14 for generating an rf signal which excites the transponder of a remote key 4 of the security system, when the key 4 is within the vicinity of the vehicle. The key 4 may comprise a card or fob. Once excited, the key 4 uses rf transmission techniques to communicate with the transceiver 14, in accordance with a secure communications protocol, in order to pass authentication data from the key 4 to the ECU 2. Once received, the ECU 2 compares the authentication data with security data that it holds in its memory, being security codes and enable flags stored in an EEPROM 12. When the ECU 2 finds a match between the received authentication data and its own security data, the ECU 2 issues signals to other components of the vehicle to enable access to and/or operation of the vehicle by a holder of the key 4. When the key 4 is removed form the immediate vicinity of the vehicle, this is detected by the transceiver 14, which causes the ECU 2 to generate signals to secure the vehicle, for example by locking and immobilising the vehicle.

Normally, a number of valid keys can be used with the security system to gain access to the vehicle. The keys 4 each include a unique serial or identification number and this is communicated to the ECU 2 as part of the authentication data. The ECU 2 stores the serial

numbers for each valid key in its EEPROM 12, and against each serial number an enable flag is stored. As an alternative to the enable flag, the system may store a control byte, which may be an encrypted version of the identification number. During the authentication procedure when the ECU 2 verifies the authentication data, the ECU 2 checks to determine if the received serial number of the communicating key 4 is stored in the EEPROM 12 and whether its enable flag is set or reset. If the serial number is found and the enable flag is set, then the communicating key constitutes a valid key which can be used to gain access to the vehicle. If however the serial number is found and the enable flag is not set, then the communicating key is no longer a valid key which can be used. The ECU 2 is able to execute a key deactivation and activation procedure which resets and sets the enable flag for keys 4. This allows an owner of the vehicle to deal with lost or stolen keys in a simple manner, as described below.

When a valid key is lost or stolen, the holder of at least one remaining valid key can place the ECU 2 in a key validation mode to validate all of the remaining keys. The holder of the remaining keys simply enters the vehicle, places all of the remaining keys within range of the transceiver 14, and executes a predetermined procedure to place the ECU 2 in the key validation mode. Once placed in the key validation mode, the ECU 2 energises all of the keys 4 within its range, to receive their serial numbers, and sets the enable flags in the EEPROM 12 for the serial numbers received, whilst resetting the enable flags for any other key serial numbers stored in the EEPROM 12. The keys that are therefore within range of the transceiver 14 will then constitute valid keys, and the lost or stolen key will no longer be a valid key, as its enable flag is reset. Completion of the key validation procedure is indicated by the ECU 2 which generates a completion signal for a message unit 6. The message unit simply indicates either visually or audibly that the key validation procedure is completed. The message unit 6 may be an LED in the vehicle or the vehicle's horn or siren. The message unit 6 may also be a display unit in the vehicle which receives and is able to display data indicating the keys which are valid for the vehicle. The display unit would also display other messages, such as "key validation completed" and can include controls which allows a user of the vehicle to recall a display indicating the valid keys, such as keys A, B and C.

When the lost or stolen key 4 is recovered, the key 4 can be revalidated or activated by again taking all of the keys into the vehicle, and placing the ECU 2 into the key validation

mode, to execute the above key validation procedure. The enable flag for the found key 4 will then be set in the EEPROM 12.

To avoid the requirement for any additional hardware components to be added to the vehicle, the predetermined procedure used to place the ECU 2 in the key validation mode needs to be executed using existing vehicle components. The predetermined procedure should advantageously involve using components and operations which are normally involved in a start or entry procedure for the vehicle. Most vehicles have a start procedure which involves pressing a pedal 8, which may be the brake or clutch pedal, and then simultaneously turning on an ignition start switch 10 of the vehicle. The ECU 2 is connected to the electrical network or wire looms of the vehicle so as to receive signals generated when the pedal 8 is depressed and the start switch 10 is turned on. The predetermined procedure to enter the key validation mode can then involve a holder of the keys simply depressing the pedal 8 and turning on the start switch 10 alternately a number of times, say three times, instead of simultaneously. The ECU 2 on detecting depression of the pedal 8 and the start switch 10 alternately can then generate a message for the message unit 6 to confirm entry into the key validation mode when the predetermined procedure has been executed. The ECU 2 can also issue cues on the message unit 6 to follow the time sequence for depression of the pedal 8 and turning on the start switch 8, to assist a holder of the keys in correctly executing the procedure to enter the key validation mode. Alternatively the steps and components used for an entry procedure for the vehicle can be used. For example, in some passive security systems the key is excited on lifting of a door handle 16. The predetermined procedure required to enter the key validation mode may require a holder of the keys to lift the door handle 16 a number of times within a period of time, say four times in two seconds.

The ECU 2 can be provided by or divided into a number of ECUs, and similarly the vehicle can include a number of transceivers and antennas to communicate with remote keys 4. The keys 4 may be passive entry keys which require energy from the vehicle in order to communicate with the ECU 2 or the keys may have their own battery power supply. Also, whilst the present invention is particularly advantageous for keys which have no activating buttons, the keys 4 can include activating buttons and the security system may be a combination active and passive security system. For example, the security system may be such that the key 4 is able to communicate over a distance, of say 30 m, with the vehicle when

activated, and is also able to be energised or excited when closer to the vehicle by lifting of a door handle, or some other activation device, when in the vicinity of the vehicle.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as herein described with reference to the accompanying drawing.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A key control method for a security system having at least one valid key and electronic control means with a transceiver for communicating with said at least one valid key, said control means generating an authority for a secure object when authentication data is received from said at least one valid key and storing unique identification data for said at least one valid key, said method including accessing said unique identification data for said at least one valid key in a mode of said system;

characterised by storing enable data corresponding to said unique identification data for said at least one valid key, a user executing a predetermined procedure to enter a key validation mode of said system, and in said validation mode retaining said enable data for valid keys within range of said transceiver and deleting said enable data for valid keys which are out of range of said transceiver, whereby keys without said enable data are deactivated for said system.

2. A key control method as claimed in claim 1, wherein said predetermined procedure includes steps of a start procedure of a vehicle.

3. A key control method as claimed in claim 1, wherein said predetermined procedure includes steps of an entry procedure of a vehicle.

4. A key control method as claimed in claim 1, wherein said predetermined procedure includes executing steps using standard controls of a vehicle.

5. A key control method as claimed in claim 4, wherein said standard controls include a brake pedal, a clutch pedal, an ignition switch, and/or a door handle.

6. A key control method as claimed in any one of claims 2 to 5, wherein said steps are executed at times relative to one another which differ from said times for standard procedures for said vehicle.

7. A key control method as claimed in any one of the preceding claims, including indicating completion of said key validation mode.

8. A key control method as claimed in claim 7, wherein said indicating includes generating a display of the activated valid keys for said system.

9. A key control method as claimed in any one of the preceding claims, wherein said keys are without activating buttons.

10. A key control method as claimed in any one of the preceding claims, wherein said enable data is a control byte.

11. A key control method as claimed in any one of claims 1 to 10, wherein said authority allows access to said secure object.

12. A key control method as claimed in claim 11, wherein said secure object is a vehicle.

13. A key control method as claimed in any one of claims 1 to 10, wherein said secure object is a vehicle and said authority allows operation of said vehicle.

14. A key control method as claimed in claim 13, wherein said operation includes starting said vehicle.

15. A security system including at least one valid key and electronic control means with a transceiver for communicating with said at least one valid key, said control means generating an authority for a secure object when authentication data is received from said at least one valid key, and storing unique identification data for said at least one valid key, said system having a mode for accessing said unique identification data for said at least one valid key;

characterised in that said control means stores enable data corresponding to said unique identification data for said at least one valid key when activated for said system, and said control means enters a key validation mode when a user executes a predetermined procedure, and in said validation mode said enable data is retained for valid keys within range of said transceiver and deleted for valid keys out of range of said transceiver.

16. A security system as claimed in claim 15, wherein said predetermined procedure

includes steps of a start procedure of a vehicle.

17. A security system as claimed in claim 15, wherein said predetermined procedure includes steps of an entry procedure of a vehicle.

18. A security system as claimed in claim 15, wherein said predetermined procedure includes executing steps using standard controls of a vehicle.

19. A security system as claimed in claim 18, wherein said standard controls include a brake pedal, a clutch pedal, an ignition switch, and/or a door handle.

20. A security system as claimed in any one of claims 16 to 19, wherein said steps are executed at times relative to one another which differ from said times for standard procedures for said vehicle.

21. A security system as claimed in any one of claims 15 to 20, including means for indicating completion of said key validation mode.

22. A security system as claimed in claim 21, wherein said indicating means includes a display of the current valid keys for said system.

23. A security system as claimed in any one of claims 15 to 22, wherein said keys are without activating buttons.

24. A security system as claimed in any one of claims 15 to 23, wherein said enable data is a control byte.

25. A security system as claimed in any one of claims 15 to 24, wherein said authority allows access to said secure object.

26. A security system as claimed in claim 25, wherein said secure object is a vehicle.

27. A security system as claimed in any one of claims 15 to 24, wherein said secure object

is a vehicle and said authority allows operation of said vehicle.

28. A security system as claimed in claim 27, wherein said operation includes starting said vehicle.

29. A vehicle including a security system as claimed in any one of claims 15 to 28.

DATED this 5th day of August, 1999

ROBERT BOSCH GmbH
By its Patent Attorneys
DAVIES COLLISON CAVE

ABSTRACT:

A key control method for a security system having at least one valid key and electronic control means with a transceiver for communicating with the at least one valid key, the control means generating an authority for a secure object when authentication data is received from the at least one valid key and storing unique identification data for the at least one valid key, the method including accessing the unique identification data for the at least one valid key in a mode of the system, characterised by storing enable data corresponding to the unique identification data for the at least one valid key, a user executing a predetermined procedure to enter a key validation mode of the system, and in the validation mode retaining the enable data for valid keys within range of the transceiver and deleting the enable data for valid keys which are out of range of the transceiver, whereby keys without the enable data are deactivated for the system.

A security system including at least one valid key and electronic control means with a transceiver for communicating with the at least one valid key, the control means generating an authority for a secure object when authentication data is received from the at least one valid key, and storing unique identification data for the at least one valid key, the system having a mode for accessing the unique identification data for the at least one valid key, characterised in that the control means stores enable data corresponding to the unique identification data for the at least one valid key when activated for the system, and the control means enters a key validation mode when a user executes a predetermined procedure, and in the validation mode the enable data is retained for valid keys within range of the transceiver and deleted for valid keys out of range of the transceiver.

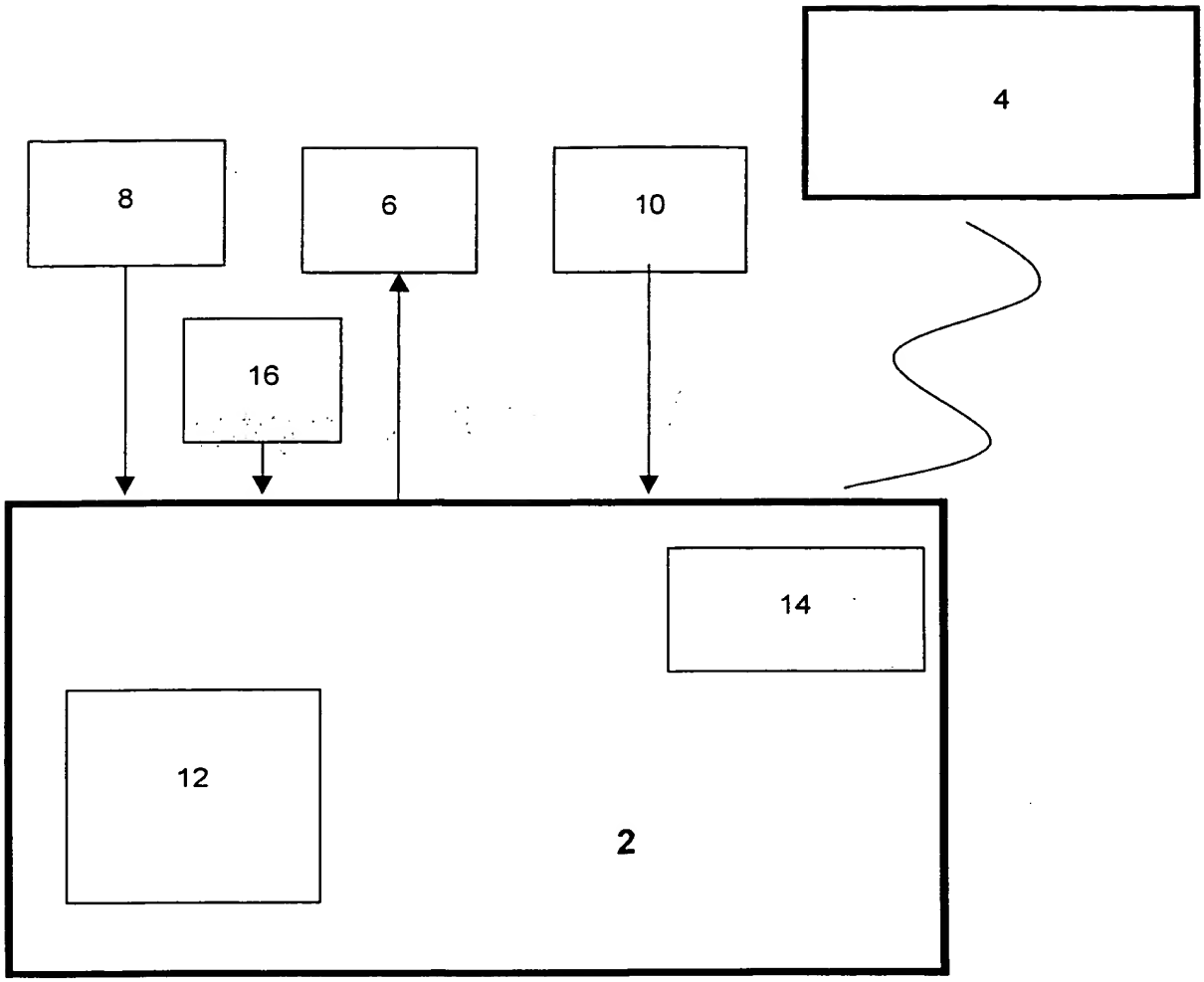


Figure 1